

**SAINT VINCENT HEALTH SYSTEM  
HIPAA BUSINESS ASSOCIATE AMENDMENT**

**This Document Is An Amendment (the “Amendment”) To An Underlying Agreement (“Underlying Agreement”) Between The Parties.** This Amendment is made by the same parties who made the Underlying Agreement identified below.

**THE UNDERLYING AGREEMENT**

**Title of Underlying Agreement:** \_\_\_\_\_

**Business Purpose of Underlying Agreement:** \_\_\_\_\_

**Date of Underlying Agreement:** \_\_\_\_\_ **Agreement No. (if applicable):** \_\_\_\_\_

**THE SAINT VINCENT COVERED ENTITY**

**The Saint Vincent entity\*** which is a party to the Underlying Agreement is referred to in this Amendment as the **“Covered Entity”** [as defined in paragraph 1(b) below]. The Saint Vincent Covered Entity is :

**Legal Name of Saint Vincent Covered Entity:** [\_\_\_\_\_]

**D/B/A:** \_\_\_\_\_  
*(complete only if the Saint Vincent Covered Entity is doing business under a name different than its legal name)*

**Name of Primary Saint Vincent Business Contact:** [\_\_\_\_\_]

**Tel #:** [\_\_\_\_\_] **Email:** [\_\_\_\_\_]

**THE VENDOR/LICENSOR/CONSULTANT/SERVICE PROVIDER**

**The Vendor/Licensor/Consultant/Service Provider** which has the Underlying Agreement with the Saint Vincent Covered Entity is referred to in this Amendment as a **“Business Associate”** [as defined in paragraph 1(a) below]. The Business Associate is:

**Legal Name of Vendor/Licensor/Consultant/Service Provider:** [\_\_\_\_\_]

**D/B/A:** \_\_\_\_\_  
*(complete only if the Business Associate is doing business under a name different than its legal name)*

**Address:** [\_\_\_\_\_]

**Name of Primary Business Contact:** [\_\_\_\_\_]

**Tel #:** [\_\_\_\_\_] **Email:** [\_\_\_\_\_]

**THE EFFECTIVE DATE**

**Effective Date of this Amendment:** Same as effective date of Underlying Agreement.

## BACKGROUND

- A. Covered Entity and Business Associate have entered into the above Underlying Agreement.
- B. Under the terms of such Underlying Agreement, Business Associate will have access to information that includes Protected Health Information (“**PHI**”)[defined in paragraph 1(e)].
- C. Covered Entity and Business Associate intend to protect a patient’s privacy and provide for the security of the PHI disclosed by Covered Entity or accessed by Business Associate pursuant to the Underlying Agreement, in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and regulations promulgated thereunder by the U.S. Department of Health and Human Services (“**HIPAA**”) and other applicable laws, including HIPAA amendments contained in the American Recovery and Reinvestment Act of 2009, Public Law 111-05 (“**The ARRA**”).
- D. HIPAA requires the Covered Entity and the Business Associate to enter into a contract (hereinafter, the “**Business Associate Amendment**” or “**Amendment**,”) containing specific requirements to protect the confidentiality and security of patients’ PHI, as set forth in, but not limited to, Title 45, Sections 164.502(e), 164.504(e) and 164.314(a)(2)(i) of the Code of Federal Regulations (“**CFR**”) and contained in this Amendment. Sections 13401(a) and 13404(a) of The ARRA require specific additional HIPAA provisions to be included in this Amendment.

## AMENDMENT

In consideration of the foregoing and the mutual promises and the exchange of information pursuant to this Amendment, the parties agree to amend the Underlying Agreement by incorporating all of the following into the Underlying Agreement:

### 1. **Definitions:**

- (a) “**Business Associate**” shall have the meaning given to such term under the Privacy Rule [defined in paragraph 1(d) below] and which includes a third party that performs functions for or on behalf of Covered Entity and has access to Covered Entity’s PHI and uses such PHI in the performance of its functions.
- (b) “**Covered Entity**” shall have the meaning given to such term under the Privacy Rule [defined in paragraph 1(d)], which includes a hospital, since it provides health care and transmits health information in electronic form in the course of its standard functions.
- (c) “**Patient**” shall have the same meaning as the term “individual” under the Privacy Rule [defined in paragraph 1(d)] and shall include a person who qualifies as a personal representative.
- (d) “**Privacy Rule**” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR 160 and 164, subparts A and E and amendments thereto.
- (e) “**Protected Health Information**” (“**PHI**”) shall have the same meaning given to such term under HIPAA and shall include any information, whether oral or recorded in any form or medium, limited to the information created or received by Business Associate from or on behalf of Covered Entity: (i) that relates to the past, present or future physical or mental condition of the patient; the provision of health care to patient; or the past, present or future payment of for the provision of health care to patient; and (ii) that identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient.
- (f) “**Facility Data**” shall mean PHI and non-PHI, disclosed or made available by or on behalf of Covered Entity to Business Associate, and shall include derivatives thereof created by Business Associate or his/her/its agents.
- (g) “**Designated Record Set**” shall have the same meaning given to such term under HIPAA and shall include patients’ medical or billing records or any group of records which contains PHI that are used, in whole or in part, by or for Covered Entity to make decisions about patients.
- (h) “**Data Aggregation**” shall have the same meaning given to such term under HIPAA and shall include the combining of PHI received or created by Business Associate to permit data analyses relating to healthcare operations of Covered Entity.
- (i) “**Secretary**” shall mean the Secretary of the Department of Health and Human Services or his designee.
- (j) “**Security Rule**” shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C, and amendments thereto.
- (k) “**Covered Account**” shall have the meaning given to such term under the FCT Fair and Accurate Credit Transactions Act of 2003 (FACTA) – “Red Flags” Rule.
- (l) “**Service Provider**” shall have the meaning given to such term under the FCT Fair and Accurate Credit Transactions Act of 2003 (FACTA) – “Red Flags” Rule.

**2. Permitted Uses and Disclosures by Business Associate**

- (a) Except as otherwise limited in the Underlying Agreement and this Amendment, Business Associate may use or disclose Facility Data only for the benefit of Covered Entity and to perform functions, activities, or services as specified in the Underlying Agreement or the minimum necessary policies and procedures of the Covered Entity. Business Associate warrants and represents that each of the data elements of any PHI that it may access or receive from or on behalf of Covered Entity is minimally necessary to permit Business Associate to provide the services under the Underlying Agreement.
- (b) Except as otherwise limited in the Underlying Agreement and this Amendment, Business Associate may use or disclose Facility Data for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that (i) the disclosure is required by law, or (ii) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that such information will remain confidential and used or further disclosed solely as required by law or for the purpose of assisting Business Associate to meet Business Associate's obligations under the Underlying Agreement.
- (c) Except as otherwise limited in the Underlying Agreement and this Amendment, Business Associate may use PHI to provide data aggregation services only for Covered Entity.

**3. Obligations of Business Associate:**

- (a) Business Associate agrees to not use or further disclose Facility Data other than as permitted or required by the Underlying Agreement, this Amendment or as required by law. As Covered Entity has not secured individual authorization from the patients whose PHI is contemplated for use under the Underlying Agreement, Business Associate is prohibited from directly or indirectly exchanging the Covered Entity's PHI for remuneration with any other person or entity, in accordance with Section 13405(d) of The ARRA.
- (b) Business Associate Protection of PHI
  - (1) Business Associate agrees to implement administrative, physical, technical and policy and documentation safeguards that reasonably and appropriately protect the privacy, security, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits under this Underlying Agreement. At a minimum, Business Associate's safeguards will include all "Required" Implementation Specifications contained in sections 164.308, 164.310, 164.312 and 164.316 of title 45 of the Code of Federal Regulations, as required by Section 13401 of The ARRA and any subsequent amendments and regulations promulgated thereunder.
  - (2) No later than the date that Section 13402 of The ARRA becomes effective, Business Associate agrees to implement and use administrative, physical and/or technical safeguards to protect Covered Entity's PHI that meet or exceed the Secretary's promulgated standards to avoid classification as "unsecured PHI". In the event Business Associate is unable to implement safeguards that avoid the classification as "unsecured PHI", Business Associate will notify Covered Entity and provide Covered Entity thirty (30) days to terminate the Underlying Agreement and this Amendment, without penalty. **If Covered Entity decides to continue with the Underlying Agreement and this Amendment after such notice, Business Associate agrees it will be solely and completely liable and responsible for all notices and notifications of Covered Entity, affected patients, and the Secretary, of any breach of PHI, in accordance with Section 13402 of ARRA, and agrees to coordinate immediately with Covered Entity in the event that notifications of a breach arising from the Business Associate is required.**
- (c) Business Associate agrees to promptly mitigate, to the extent practicable, any harmful effect of a use or disclosure of Facility Data by Business Associate in violation of the Underlying Agreement and this Amendment.
- (d) Business Associate agrees to establish and implement a system of sanctions for any employee, agent or subcontractor who violates the Amendment or the HHS Privacy Regulations. (ref. 45 CFR 164.530(e)(1).)
- (e) Business Associate Notice to the Covered Entity of Non-Authorized Use, Disclosure Access or Breach of PHI
  - (1) Business Associate agrees to promptly report to Covered Entity any use or disclosure of Facility Data not provided for by the Underlying Agreement and/or this Amendment, including any requests for inspection, copying or amendment of such information and including any security incident involving Facility Data. Business Associate shall maintain a record of all such requests for inspection, copying and amendment(s) of Facility Data not provided for by the Underlying Agreement, including those initiated by Patient, Covered Entity, or third parties, and to promptly provide such documentation to Covered Entity upon request.
  - (2) Business Associate agrees to promptly notify the Covered Entity of any breach of any unsecured PHI of the Covered Entity in its possession, but in any event no later than sixty (60) days of the occurrence of the breach, as required by Section 13402(b) of The ARRA. The content of the Business Associate notice to the Covered Entity shall conform to the requirements of Section 13402(b) of The ARRA and any subsequent amendments and resulting regulations.

- (f) Business Associate agrees to ensure in writing that any agent, including a subcontractor, to whom it provides Facility Data agrees to the same restrictions and conditions that apply to Business Associate with respect to such information, including appropriate and comparable safeguards, as defined in paragraph 3(b), above. Notwithstanding the foregoing or anything to the contrary in the Underlying Agreement or this Amendment, Business Associate shall not use any agent or subcontractor to perform any service under the Underlying Agreement without the express written consent of an authorized representative of the Covered Entity and only after such agent or subcontractor has agreed in writing to comply with the same restrictions and conditions that apply to Business Associate under the Underlying Agreement and this Amendment with respect to such information.
- (g) Access to Facility Data held by Business Associate and Business Associate Accounting for Disclosures
  - (1) Business Associate agrees to provide prompt access to Facility Data in designated record sets to Covered Entity whenever so requested by Covered Entity, or, if directed by Covered Entity, to a Patient in order to meet the requirements of HIPAA. If Patient requests directly from Business Associate (i) to inspect or copy his or her PHI, or (ii) requests its disclosure to a third party, the Business Associate shall promptly notify Covered Entity's facility privacy official of such request and await such official's denial or approval of the request.
  - (2) After the date that Covered Entity informs Business Associate that Covered Entity has implemented an Electronic Health Record, Business Associate shall provide, in response to a request from an individual, an accounting of all disclosures the Business Associate made in the past three years of the individual's PHI.
- (h) Business Associate agrees to promptly make amendment(s) to Facility Data requested by Covered Entity and shall do so in the time and manner requested by Covered Entity to enable it to comply with HIPAA. If Patient requests an amendment to his or her PHI, directly from Business Associate, the Business Associate shall promptly notify Covered Entity's facility privacy official of such request and await such official's denial or approval of the request.
- (i) Business Associate agrees to promptly make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate for or on behalf of, Covered Entity available to the Covered Entity or the Secretary, in a time and manner designated by the Covered Entity or Secretary, to enable the Secretary to determine compliance with HIPAA, and to cooperate fully with any HIPAA audit of the Business Associate that the Secretary may undertake under Section 13411 of The ARRA, or that the Covered Entity undertakes to assure compliance.
- (j) Business Associate agrees to document and provide to Covered Entity all disclosures of Facility Data and information related to such disclosures, and shall do so in the time and manner designated by Covered Entity, to enable it to meet HIPAA requirements for an accounting of such disclosures.
- (k) Business Associate agrees to cooperate with the Covered Entity and its medical staff to preserve and protect the confidentiality of Facility Data accessed or used pursuant to the Underlying Agreement and will not disclose or testify about such information during or after the termination of the Underlying Agreement, except as required by law.
- (l) As required by the FTC Fair and Accurate Credit Transactions Act of 2003 (FACTA) "Red Flags" Rule, to the extent that the Business Associate is a Service Provider (within the meaning of the Red Flags Rule) performing an activity for the Covered Entity in connection with one or more Covered Accounts, the Business Associate shall employ policies and procedures to detect relevant Red Flags that might arise in the performance of the Business Associate's activities and shall take appropriate steps to prevent or mitigate identity theft.

**4. Obligations of Covered Entity**

- (a) Covered Entity shall notify Business Associate of any limitation in its notice of privacy practices in accordance with 45 CFR 164.520 to the extent that such limitation may affect Business Associate's permitted use or disclosure of PHI.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Patient to the use or disclosure of PHI, to the extent such changes affect Business Associate's permitted or required uses and disclosures of PHI.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to the extent that such restriction may affect Business Associate's permitted use or disclosure of PHI.
- (d) Covered Entity shall notify Business Associate of the date it will implement an electronic medical record to permit Business Associate to implement its accounting for disclosure obligation per paragraph 3.(g)(2) above. Notice of the implementation status of various members of the Saint Vincent family of entities can be found online by going to [www.saintvincenthealth.com](http://www.saintvincenthealth.com) and clicking "Vendors" or by contacting your Saint Vincent primary business contact.

**5. Effect of Breach of Obligations**

- (a) Should Business Associate breach any of its obligations herein, Covered Entity shall have the option to either:
- (1) Provide Business Associate an opportunity to cure the breach and end the violation within the time specified by Covered Entity. If Business Associate does not cure the breach or end the violation as specified by Covered Entity, Covered Entity may terminate its obligations to Business Associate, including, but not limited to, its payment obligations and obligations to provide information, materials, equipment or resources to Business Associate; or
  - (2) Immediately terminate this Underlying Agreement, without prejudice to other legal remedies available to Covered Entity.
  - (3) If neither termination nor cure is feasible, Covered Entity may report the violation to the Secretary.
- (b) Separate and apart from any action the Covered Entity may take in the event of a breach, Business Associate understands that the Secretary, or the Department of Justice, may impose civil or criminal penalties directly against a Business Associate for failure to comply with the HIPAA requirements and standards (under 42 USC §1320d-5) or for wrongful disclosure of individually identifiable health information (under 42 USC§1320d-6), as required by Sections 13401(c) and 13404(c) of The ARRA.

**6. Effect of Termination**

- (a) Upon termination of this Underlying Agreement, Business Associate shall promptly return to Covered Entity all Facility Data, including derivatives thereof or, upon Covered Entity's request, destroy such data. This provision shall apply to Facility Data in the possession of subcontractors or agents of Business Associate. Upon destruction of Facility's Data, Business Associate shall certify in writing that such information has been destroyed. Notwithstanding the foregoing, Business Associate shall notify Covered Entity in writing about its intent to destroy data within ten (10) days before such date of destruction. If Covered Entity requests the return of any Facility Data, Business Associate shall comply as requested.
- (b) If the return or destruction of Facility Data is infeasible, Business Associate shall promptly notify Covered Entity of the conditions that make such return or destruction infeasible. Upon mutual determination by the parties that return or destruction of Facility Data is unfeasible; Business Associate shall extend the protections of this Amendment to such data and shall limit its further use or disclosure to purposes that make its return or destruction infeasible.

**7. Indemnity**

Business Associate shall promptly and fully defend, indemnify and hold harmless Covered Entity, its affiliates and respective officers, directors, agents and employees against all claims, demands and judgments made or recovered against them for damages relating to a violation of the Privacy or Security Regulations regarding access to, use or disclosure of PHI, to the extent that such violation was caused by an action or omission of Business Associate, its subcontractor or its employees or agents.

**8. General**

Except as amended by this Amendment, all other terms of the Underlying Agreement remain in full force and effect. The Underlying Agreement and this Amendment and attachments thereto are intended to be read and construed in harmony with each other, but in the event that any provision in this Amendment conflicts with the provisions of the Underlying Agreement or other attachments, the provisions in this Amendment shall be deemed to control, and such conflicting provision or part thereof shall be deemed removed and replaced with the governing provision herein.

**AGREED AND ACCEPTED:**

<b>Name of Saint Vincent Covered Entity:</b> [ _____ ] _____ Authorized Signature [ _____ ] Print Name [ _____ ] Print Title _____ Date	<b>Name of Business Associate:</b> [ _____ ] _____ Authorized Signature [ _____ ] Print Name [ _____ ] Print Title _____ Date
--	--

\* The Saint Vincent “family” of entities consists of the parent Saint Vincent Health System, together with Saint Vincent Health Center, Saint Vincent Surgery Center, Saint Vincent Medical Group, Saint Vincent Foundation, Rehab Solutions and others. Because of the common ownership and control of these entities, they have designated themselves as a single “affiliated entity” for purposes of simplifying compliance with HIPAA. The blanket term “Saint Vincent” should be understood to refer to the specific entity(ies) in the family with which you have a relationship. For a detailed listing of Saint Vincent’s “family,” you should visit the Saint Vincent website at [www.saintvincenthealth.com](http://www.saintvincenthealth.com), click on “privacy policy” and select the “notice of privacy practice document.” This link will be updated regularly to reflect any changes in the Saint Vincent Health System “family.”